We Claim:

1. A method of providing digital data from a source system to an embedded system in a secure manner, comprising the steps of:
combining the data with header information including a target identifier corresponding to the embedded system;
providing the combined digital data with header information to the embedded system; and
verifying the target identifier before the embedded system is enabled to load the digital data.
2. The method as defined in claim 1 wherein the target identifier is a text name corresponding to an end user of an Internet based service.
3. The method as defined in claim 1 wherein said target identifier includes a revision level respecting said digital data.
4. A method of providing digital data from a source system to an embedded system in a secure manner, comprising the steps of:
combining the data with header information including a target identifier corresponding to the embedded system;
signing the combined digital data with header information with a digital signature corresponding to the source system, the digital signature being added to the header information
providing the combined digital data with header information to the embedded system; and
verifying the digital signature and the target identifier before the embedded system is enabled to load the digital data.
5. The method as defined in claim 4, wherein the step of signing the combined digital data with header information uses a private cryptographic key associated with the source system to generate the digital signature.

6. The method as defined in claim 5 wherein the step of verifying the digital signature uses a public key corresponding to the private cryptographic key.

7. An embedded system that uses a target state header to validate uploaded files the system comprising:
means to combine the files to be uploaded with the target state header;
means to provide the files with the target state header to the embedded system; and
verifying means to verify the target state header before the files are uploaded to the embedded system.

8. The embedded system as defined in claim 7 having means to provide a digital signature for use in verifying the files before uploading to the embedded system.

9. The embedded system as defined in claim 8 having public keying infrastructure for distributing public keying information to said embedded system.

10. The embedded system as defined in claim 9 having software for performing signature generation and verification.

11. The embedded system as defined in claim 7 for use in conducting transactions on the Internet.

12. The embedded system as defined in claim 11 wherein said transactions include the purchase and download of software.

13. The embedded system as defined in claim 11 wherein said transactions include online banking.

14. The embedded system as defined in claim 11 wherein said transactions include the installation of software revisions in network nodes.

15. The embedded system as defined in claim 11 wherein said network nodes include wireless telephones.